

ALLIGATE仕様書

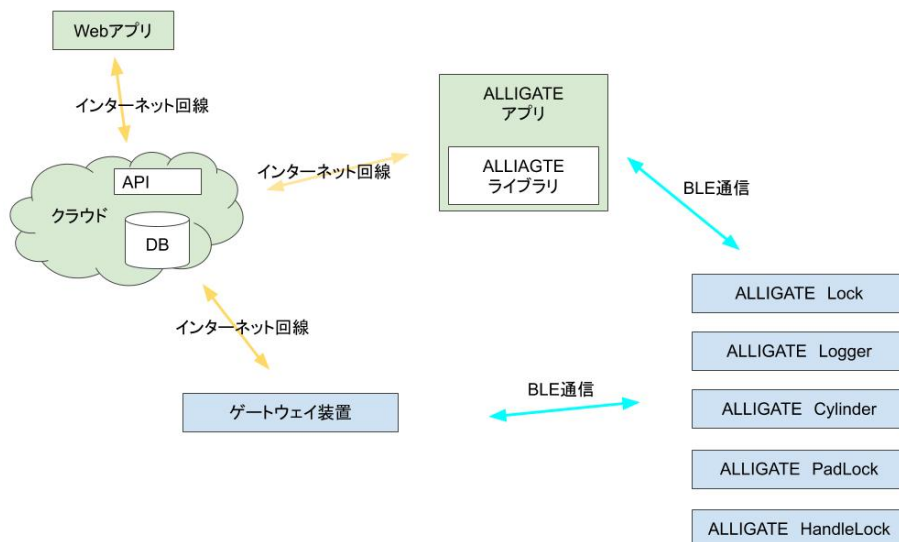
ALLIGATE機能仕様

1. 概略

本システムは、アクセスコントロールプラットフォームサービス「ALLIGATE」の機能を示す仕様書とする。システムは、クラウド・Webアプリ・スマホアプリ・カードリーダーで構成され、アクセスコントロール機能を実現している

2. システム構成

2-1. システム構成図



2-2. 用語の定義

ALLIGATEシステム	本システムの機能全体を示す
Webアプリ	Webブラウザで動作するクラウド管理ツール
クラウド	システム全体の情報を管理するサーバ群
API	Webアプリ以外でクラウド管理を行うための開発用ツール
DB	クラウドの情報を永続的に保存しているデータベース
ALLIGATEアプリ (スマホアプリ)	各端末措置を利用・設定・クラウドとの通信をするためのAndroid/iOS用のスマホアプリ
ALLIGATEライブラリ (SDK)	ALLIGATEアプリ以外で各端末装置を利用・設定・クラウドとの通信をするための開発用ツール
ゲートウェイ装置	クラウドと各端末装置の通信を行うための装置 Cube for ALLIGATE: ハードウェアでこの機能を有する装置 ALLIGATE Way: ソフトウェアでこの機能を有するiOS用のスマホアプリ
各端末装置	以下の端末装置の総称 入退室管理装置: ALLIGATE Lock 入退室管理装置: ALLIGATE HandleLock

	入退室管理装置：ALLIGATE CylinderLock スマート南京錠：ALLIGATE PadLock 出退勤記録装置：ALLIGATE Logger
端末装置／装置	各端末装置のいずれかを示す
照合	端末装置に対して認証をする行為 照合を行い認証が通ると鍵の解錠等が行われ入室できる状態とな理、照合ログが発生する（ALLIAGTE Loggerは照合ログの発生のみ実施される）
デバイス	端末装置に対して、照合を行うためのカードやテンキー、スマホアプリを示す
テンキー	端末装置に対して、総合を行うためのデバイスのうち、任意の桁数の番号を入力することで照合を行う行為 ALLIGATE Lockのオプションリーダーのみこの機能を有する
適応デバイス	ALLIGATEシステムで各端末装置と照合可能なデバイス
利用者 (ユーザー)	適応デバイスを有して端末装置を利用するALLIGATEシステムの利用者。オフィスで利用する際は社員全般を指す
アカウント	利用者が、ALLIGATEシステム（WebアプリとALLIGATEアプリ）へログインするための情報
ゲート	Webアプリ・ALLIGATEアプリでの端末装置の別名

2-3. 動作環境について（推奨環境）

(1) Webアプリ（実行環境のWebブラウザ）

- 1) GoogleChrome 88.0以上（最新バージョン推奨）
- 2) スマートホン・各種Pad製品は非推奨

(2) 適応デバイス：ALLIGATEアプリ（実行環境のスマートフォン）

- 1) Apple製品iOS Ver11.00以上
- 2) Android各種製品

- a. OSはVer8.0以上
- b. BLEVerは4.3以上

(3) 適応デバイス：NFCカード

FeliCa , MIFARE

(4) 適応デバイス：NFC搭載デバイス

以下、ALLIGATE Lock / Logger のみ対応

- a. iPhoneのApple Pay：交通系ICカードアプリNFC
- b. Androidのおサイフケータイ：交通系ICカードアプリ

2-4. 通信方式

送信元	送信先	通信方式	ポート：プロトコル
Webブラウザ	クラウド	インターネット	443：HTTPS
ALLIGATEアプリ	クラウド	インターネット	443：HTTPS

			8883 : MQTTS
ゲートウェイ装置 (Cube for ALLIGATE)	クラウド	インターネット (LTE)	443 : HTTPS 8883 : MQTTS
ゲートウェイ装置 (ALLIGATE Way)	クラウド	インターネット	443 : HTTPS 8883 : MQTTS
ALLIGATEアプリ	各端末装置	Bluetooth	独自暗号化通信
ゲートウェイ装置 (Cube for ALLIGATE)	各端末装置	Bluetooth	独自暗号化通信
ゲートウェイ装置 (ALLIGATE Way)	各端末装置	Bluetooth	独自暗号化通信
NFCカード	各端末装置	NFC	—
NFC搭載デバイス	各端末装置	NFC	—

3. 入退室管理システム

3-1. 標準機能

(1) クラウドでのデータ管理

以下の全てのデータはクラウドにて管理され、Webアプリにより登録・編集・参照などを行うことができる。

- 利用者（ユーザー）情報
- カード情報
- 利用者（ユーザー）とカード情報の紐付け
- ALLIGATEアプリが入っているスマホ端末情報
- ゲートの名称や電波強度、照合音などの設定情報
- その他、システム設定情報

以下の全ての設定は、クラウドで管理され、適切なタイミングでALLIGATEアプリや（ゲートウェイ装置もしくはスマホアプリを経由して）各端末装置と通信を行う。

- 利用者（ユーザー）、カード情報の有効化・無効化
- 入退室権限
(常時利用できる権限、一時利用権限、帰還指定の権限)
- ゲート設定
- ファームウェア配信

(2) 利用者（ユーザー）の権限管理

利用者の持つアカウントには以下の3つの権限を付与することができる

- * どの権限も付与されていない場合、一般の利用者として
[端末装置への照合]、[自分自身の入退室ログの閲覧]のみが行える。

1) 組織管理権限

全ての[クラウドでのデータ管理]を実施することができる

2) ゲート設定権限

[クラウドでのデータ管理]の内、クラウドの設定情報を端末装置に通信することができる

* 設定をすることはできないが、設定を適応することができる

3) 鍵共有権限

自身のアカウントの入退室権限で利用できる設定になっている端末装置に対して、ALLIGATEアプリを使って一定時間のみ、もしくは1回だけ利用できる権限を別の利用者、もしくはアカウントを有しない非利用者へ貸与することができる

(3) 各端末装置 (ALLIGATE Lock, Logger, CylinderLock, HandleLock, PadLock) の利用 適切な権限が与えられて許可された各種デバイス (カード・スマホアプリ・テンキー等) により操作することにより動作する

1) カード及びテンキーは装置に登録された情報と照合する

2) スマホアプリは、クラウドより取得した有効期限付きの権限情報を装置へ送信し、権限情報が有効期間内であるかも含めて照合する

(有効期間は、照合権限の期間と、ダウンロードした鍵の有効期限がある)

(4) クラウドと各端末装置の通信

各端末装置は、ゲートウェイ装置 (Cube for ALLIGATE) もしくはスマホアプリ (ALLIGATE Way) により自動的に以下のクラウドとの通信を行う。

* これらの通信はALLIGATEアプリで、手動で行うことも可能

➤ クラウドに登録されたカードを各種端末装置へ送信する

➤ クラウドで設定した端末設定 (照合音の種類・電波強度など) を各種端末装置へ送信する

➤ 各端末装置で発生した入退室履歴をクラウドへ送信する

(5) 各端末装置への照合

適応デバイスにて、照合を行うことで、鍵を解錠して入室退室を行い、そのログを発生させることができる。(ALLIGATE Loggerについてはログの発生のみ)

照合方法は、ALLIGATEアプリを利用する場合はアプリ起動後に対象の端末装置名のアイコンをタップ操作することで照合する。それ以外のNFCカード・NFC搭載デバイスに関しては端末装置の照合部分にカードやスマホをかざすことで照合する。

※一部動作保証しないデバイスがあります

(6) ALLIGATEアプリのログイン制限

ALLIGATEアプリへログインすることができるスマホの台数を設定することができる。

また、ALLIGATEアプリへログインする際に、組織管理者権限を持つアカウントでログインしている利用者の許可がないと利用できないように制限することができる

(7) 端末装置の照合での2段階認証

端末装置への照合を2段階で認証することができる。

デバイスにALLIGATEアプリを使用する場合、タップ操作のあと、任意の暗証番号を入力して照合する。（全ての端末機器に対応）

それ以外のNFCカード・NFC搭載デバイスに関しては端末装置の照合部分にカードやスマホをかざした後、任意の暗証番号を端末装置のテンキーへ入力することで照合する。（テンキー付きのALLIGATE Lockのみ対応）

（８）各端末装置の管理

組織管理権限を持つアカウントにより、クラウドでの各端末装置の設定を行うことができる。

また、ゲート設定権限を持つアカウントにより、その設定を適応することができる。

（９）ゲートパスワード

テンキー付きのALLIGATE Lockにて、任意の期間で、定期的に変わるパスワードで照合できる機能を利用することができる。

パスワードの有効期間は４つの時間を指定することが可能で、１つの時間帯で１００種の照合可能なパスワードが設定され、その時間内だけ有効なパスワードとして機能する。現在時間の有効なパスワードはWebアプリにて組織管理権限のアカウントで取得することができる。

３－２．オプション機能

（１）外部ログイン

利用者のアカウントに紐付けてソーシャルログイン（Googleアカウント、Appleアカウント）、SAML認証でのログイン（OneLogin）でWebアプリ・ALLIGATEアプリにログインすることができる。

（２）SMSによる２段階認証

利用者のアカウントでWebアプリ・ALLIGATEアプリにログインする際にアカウント情報入力後に、SMSで認証コードを受け取りコード入力後にログインすることができる機能。

３－３．ALLIGATE Lockの機能

【機能】

- （１）許可されたデバイスで操作することにより、電気錠を解錠することができる。
- （２）カードは最大12,000名登録することができる。
- （３）操作したログは装置に最大16,000件保存することができる。
- （４）電気錠制御は、電気錠制御盤により行われ、火災信号・インターホン連動が行える。
- （５）電気錠制御盤の盤面から電気錠を連続的に解錠状態にすることができる。
- （６）電気錠のエラー（開扉警報・施錠解錠エラー・こじ開け）時にはブザーが鳴動するとともに、警報の出力をすることが可能。
- （７）警備連動機能として、警備セット中にはカード操作を禁止することが可能。

- (8) アンチパスバック機能を利用することができる
- (9) クラウド (Webアプリ) から遠隔解錠をすることができる

3-4. ALLIGATE Loggerの機能

- (1) 許可されたデバイスで操作することにより、照合したログを残すことができる。
- (2) カードは最大12,000名登録することができる。
- (3) 操作したログは装置に最大16,000件保存することができる。

3-5. ALLIGATE CylinderLockの機能

- (1) 許可されたデバイスで操作することにより、照合したログを残すことができる。
- (2) カードは最大2,000名登録することができる。
- (3) 操作したログは装置に最大1,000件保存することができる。
- (4) デバイスで照合すると、空転しているシリンダー一部が固定され鍵のデットボルトを操作することができ、手動で鍵の施錠・解錠を行うことができる。
- (5) 照合操作後、5秒経過するとシリンダー一部は空転し施錠・解錠が出来なくなる。

3-6. ALLIGATE HandleLock

- (1) 許可されたデバイスで操作することにより、照合したログを残すことができる。
 - 1) カードは最大2,000名登録することができる。
- (2) 操作したログは装置に最大1,000件保存することができる。
- (3) デバイスで照合すると、空転しているレバーハンドルが固定され解錠することができる。
- (4) 照合操作後、5秒経過するとレバーハンドルが空転して解錠できなくなる。

3-7. ALLIGATE PadLock

- (1) 許可されたデバイスで操作することにより、照合したログを残すことができる。
- (2) カードは最大2,000名登録することができる。
- (3) 操作したログは装置に最大1,000件保存することができる。
- (4) デバイスで照合すると、空転しているシリンダー一部が固定され南京錠を解錠することができる。
- (5) 照合操作後、5秒経過するとシリンダー一部は空転する。
- (6) 南京錠の施錠は手動にて行う。

4. 管理ソフト（Webアプリ）の機能

Webアプリは権限によって利用できる機能が制限される

4-1. Webアプリのダッシュボードの機能（全権限共通）

（1）アカウント管理

- 1）認証に必要な情報（事業者ID・ユーザーID・パスワード）を入力してログインする
- 2）外部ログインを利用してログインする
- 3）ログインの際にSMSによる2段階認証を利用する
- 4）SMSによる2段階認証を利用している場合、SMS用の電話番号の設定ができる
- 5）ログインした自身のアカウントのパスワード変更ができる

4-2. Webアプリのダッシュボードの機能（組織管理権限）

（1）ユーザー管理

- 1）ユーザーの登録・修正・閲覧を行うことができる
- 2）2段階認証用の暗証番号を設定することができる
- 3）入退室権限（どのゲートへ入室許可するか）の設定をすることができる
- 4）カードを登録してユーザーへ紐付けることができる（複数のカードの紐付けが可能）
- 5）CSVファイルで一括登録することができる
- 6）期限付き入退室権限として、利用開始日時・利用終了日時の設定ができる
（ALLIGATEアプリでの照合のみ適応可能）
- 7）ユーザーを無効（利用不可）、有効（利用可能）にすることができる

（2）ゲート管理

- 1）ゲート（端末装置）に対して任意の名前を設定することができる
- 2）ゲートの設定（照合音、電波強度）の設定をすることができる
- 3）ゲートパスワードの設定をすることができる
- 4）ゲートを無効（利用不可）、有効（利用可能）にすることができる

（3）カードの管理

- 1）利用者に対して複数のカードの割当が可能
- 2）CSVファイルから利用するカード情報を一括で登録することが可能
- 3）カードを無効（利用不可）、有効（利用可能）にすることができる

（4）入退室設定のグループ設定

- 1）複数のゲートと複数のユーザーを任意のグループに紐づけることで入退室設定をグループ管理する
- 2）1つのゲートは複数のグループに紐づけることができる
- 3）1つのユーザーは複数のグループに紐づけることができる
- 4）グループを無効（利用不可）、有効（利用可能）にすることができる

- (5) ALLIGATEアプリを利用しているスマートフォンの管理
 - 1) ALLIGATEアプリを利用（ログイン）しているスマートフォンを無効（利用不可）、有効（利用可能）にすることができる
- (6) 入退室履歴の管理
 - 1) 入退室履歴を時系列で閲覧することが可能
 - 2) 期間指定、条件設定等の絞り込みが可能
 - 3) 表示する項目のフィルターが可能
 - 4) CSVファイルとして外部へ出力することが可能
- (7) 操作履歴（監査ログ）の管理
 - 1) Webアプリでの操作履歴を時系列で閲覧することが可能
 - 2) 期間指定、条件設定等の絞り込みが可能
 - 3) 表示する項目のフィルターが可能
 - 4) CSVファイルとして外部へ出力することが可能
- (8) 鍵共有機能
 - 1) 自身のアカウントの入退室権限で利用できる設定になっている端末装置に対して、ALLIGATEアプリを使って一定時間のみ、もしくは1回だけ利用できる権限を別の利用者、もしくはアカウントを有しない非利用者へ貸与することができる。
- (9) ALLIGATEの導入開始時に行う設定
 - 1) NFC読み出し位置の設定
 - 2) キートークン有効期間の設定
 - 3) スマートフォン自動認証の設定（管理者が許可が必要かどうかの設定）
 - 4) 照合種別設定（入退室履歴のログ名称の変更が可能）

4-3. Webアプリのダッシュボードの機能（組織管理権限を有していないアカウント）

- (1) 入退室履歴の管理
 - 1) ログインした利用者自身の入退室履歴を時系列で閲覧することが可能（過去30日分のみ）
 - 2) 表示する項目のフィルターが可能

5. ALLIGATEアプリ（スマホアプリ）の機能

ALLIGATEアプリは権限によって利用できる機能が制限される

5-1. ALLIGATEアプリ（スマホアプリ）の機能（全権限共通）

- (1) カードリーダーのBLE検出範囲内で、かつその端末装置に対して入退室権限が付与されていればゲートアイコンをタップして照合することができる
- (2) よく利用する端末装置を「お気に入り」として登録することができる
- (3) 圏内のみ、圏外、お気に入りゲートアイコンの表示を切り替えることができる

- (4) 自分自身の入退室履歴が参照できる
- (5) 複数のアカウントの管理が可能

5-2. ALLIGATEアプリ（スマホアプリ）の機能（ゲート管理権限）

- (1) 端末装置のファームウェアアップデートを行うことができる
- (2) クラウドに設定されている端末装置の設定情報を端末装置へ適応することができる
- (3) クラウドに登録されているカード情報を端末装置へ適応することができる

5-3. ALLIGATEアプリ（スマホアプリ）の機能（鍵共有権限）

- (1) 鍵共有を行うことができる

5-4. 他社システムとの連携について

- (1) 以下のクラウド勤怠管理システムに対して、入退室履歴データを勤怠データとして連携させることができる。

1) TeamSpirit/ジョブカン/キングオブタイム/e-就業 2020年3月現在

- (2) HR管理システムに対して、HRシステム側で登録・設定したデータをALLIGATEの利用者として登録・変更・削除することが出来ます

a. SmartHR 2020年3月末現在

※連携されるシステム製品及び詳細資料はALLIGATEのHP (<https://alligate.me>) を参照

改定履歴

図番	内容	備考
S06014-01-09325	初版	
AL03-001-210304	第二版	

- ・ARTロゴは、株式会社アートの登録商標である。
 - ・Microsoft、Windowsは、米国Microsoft Corporationの米国およびその他の国における登録商標また商標である。
 - ・Intel、Pentiumはアメリカ合衆国およびその他の国におけるインテルコーポレーションおよび子会社の登録商標または商標である。
 - ・Apple、Apple Pay、Apple Watch、iPad、iPad Pro、iPhone、Safari、Touch IDは、米国および他の国々で登録されたApple Inc.の商標です。iPhoneの商標は、アイホン株式会社のライセンスにもとづき使用されています。App Store、AppleCare、iCloud、iTunes Storeは、Apple Inc.のサービスマークである
 - ・Bluetooth® は米国Bluetooth SIG, Inc.の登録商標である
 - ・Google および Google ロゴ および G ロゴ、Android および Android ロゴ、Google Play (旧 Android マーケット) および Google Play ロゴ、Google Chromeは、Google LLCの商標または登録商標である
- その他記載されている会社名、製品名は、各社の登録商標または商標である。